

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

SIDDHARTH MEHTA, et al.,

Plaintiffs,

v.

ROBINHOOD FINANCIAL LLC, et al.,

Defendants.

Case No. 21-cv-01013-SVK

**ORDER GRANTING IN PART AND
DENYING IN PART DEFENDANTS'
MOTION TO DISMISS**

Re: Dkt. Nos. 15, 17, 22

I. INTRODUCTION

Defendants Robinhood Financial LLC and Robinhood Securities, LLC (“Defendants” or “Robinhood”) move to dismiss Plaintiffs Siddharth Mehta (“Mehta”), Kevin Qian (“Qian”), and Michael Furtado’s (“Furtado”) (collectively, “Plaintiffs”) First Amended Class Action Complaint (“FAC”) (Dkt. 10) pursuant to Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim upon which relief can be granted and Rule 9(b) on the grounds that Plaintiffs fail to plead some claims with the particularity required by Rule 9(b). Dkt. 15. The Parties have consented to the jurisdiction of a magistrate judge. Dkts. 9, 14.

The Court held a hearing on April 27, 2021. Dkt. 29. After considering the Parties’ submissions, arguments at the hearing, the case file and relevant law, the Court **GRANTS IN PART AND DENIES IN PART** Defendants’ motion to dismiss the FAC for the reasons discussed below.

II. BACKGROUND

This discussion of the background facts is based on the allegations of Plaintiffs’ FAC. Plaintiffs allege that Robinhood failed to keep their promise to maintain the highest security standards. Dkt. 10 ¶ 15. As a result, in the summer and fall of 2020, and perhaps even earlier,

1 unauthorized users accessed approximately 2,000 Robinhood customers' accounts containing the
 2 customers' sensitive personal and financial information and looted their funds. *Id.* ¶¶ 4, 18.
 3 Plaintiffs allege that Robinhood does not offer a phone number for customer service, forcing
 4 customers to attempt to contact Robinhood by email. *Id.* ¶¶ 4, 21. Robinhood customers were left
 5 waiting for days or weeks while their account funds were depleted. *Id.* ¶¶ 4, 21. Plaintiffs further
 6 allege that Robinhood failed to freeze the affected accounts or alert their customers of the breach
 7 right away and did nothing until news outlets reported on the breach. *Id.* ¶¶ 5, 20. After the
 8 security breaches were widely reported, Robinhood sent push notifications to customers
 9 encouraging them to enable two-factor authentication. *Id.* ¶ 20. Plaintiffs allege that many
 10 individuals who were affected by the breach already had two-factor identification enabled when
 11 the unauthorized access occurred. *Id.* Collectively, Robinhood customers lost millions of dollars
 12 and have spent substantial amounts of their time attempting to remedy the losses and prevent
 13 further losses. *Id.* ¶¶ 18, 22, 23. Plaintiffs allege that while Robinhood promised it would cover
 14 100 percent of any losses due to unauthorized activity, Robinhood has only compensated some
 15 individuals while refusing other individual's requests. *Id.* ¶¶ 6, 22.

16 Plaintiff Mehta held an investment account with Robinhood and was a purchaser of their
 17 services in 2020. *Id.* ¶ 27. As early as July 22, 2020, or possibly sooner, there was unauthorized
 18 access to Mehta's personal and financial information, funds Mehta had deposited into a
 19 Robinhood account, and control of securities positions Mehta purchased through Robinhood. *Id.*
 20 As a result of Robinhood's negligent and illegal conduct, Mehta lost tens of thousands of dollars
 21 and "spent hours of his own time attempting to research and remedy the loss and securing his
 22 other assets and information from further breach." *Id.* Robinhood did not inform Mehta of this
 23 breach and only acknowledged the breach after Mehta confronted Robinhood about the loss of
 24 funds 85 days after the initial breach occurred. *Id.*

25 Similarly, Plaintiff Qian held an investment account with Robinhood and was a purchaser
 26 of their services in 2020. *Id.* ¶ 28. As early as October 10, 2020, and possibly sooner, there was
 27 unauthorized access to Qian's personal and financial information, access to funds he had deposited
 28 into a Robinhood account, and control of securities positions he had purchased through

Robinhood. *Id.* Plaintiffs allege that Robinhood neglected to inform him of this breach and only acknowledged the breach after Qian confronted Robinhood about the loss days after the initial breach. *Id.* As a result, Qian has also lost tens of thousands of dollars and spent hours of his own time attempting to research and remedy the loss and protect his assets and information from further breach. *Id.*

Plaintiff Furtado held an investment account with Robinhood and was a purchaser of their services in 2021. *Id.* ¶ 29. As early as February 12, 2021 and possibly sooner, there was unauthorized access to Furtado's personal and financial information, access to the funds he had deposited into a Robinhood account, and control of securities positions Furtado purchased through Robinhood. *Id.* Furtado attempted to contact Robinhood by email, because Robinhood does not provide a customer service phone number. *Id.* However, he did not receive a response regarding the breach for thirteen days. *Id.* As a result, Furtado lost over ten thousand dollars, purchased identity theft protection services, and has spent time attempting to research and remedy the loss and protect his assets and information from further breach. *Id.*

Plaintiffs bring this action to seek monetary and equitable relief as a class action on behalf of themselves and the following classes:

Class: All Robinhood customers whose accounts were accessed by unauthorized users from January 1, 2020 to the present.

Reimbursement Subclass: All Class members who suffered direct losses due to unauthorized activity and were not compensated in full by Robinhood for said losses.

California Subclass: All Class members who were California residents.

Id. ¶¶ 34-36.

III. REQUEST FOR JUDICIAL NOTICE AND INCORPORATION BY REFERENCE

A. Legal Standard

There are two doctrines that allow district courts to consider material outside the pleadings without converting a motion to dismiss into a motion for summary judgment: judicial notice under Federal Rule of Evidence 201 and incorporation by reference. *Khoja v. Orexigen Therapeutics*,

1 *Inc.*, 899 F.3d 988, 998 (9th Cir. 2018), *cert. denied sub nom. Hagan v. Khoja*, — U.S. —, 139 S.
 2 Ct. 2615, 204 L. Ed. 2d 264 (2019). “The court may judicially notice a fact that is not subject to
 3 reasonable dispute.” Fed. R. Evid. 201(b). A fact is “not subject to reasonable dispute” if it “is
 4 generally known” or “can be accurately and readily determined from sources whose accuracy
 5 cannot reasonably be questioned.” Fed. R. Evid. 201(b)(1)-(2). However, “[j]ust because the
 6 document itself is susceptible to judicial notice does not mean that every assertion of fact within
 7 that document is judicially noticeable for its truth.” *Khoja*, 899 F.3d at 999.

8 Incorporation by reference is a judicially created doctrine that allows a court to consider
 9 certain documents as though they are part of the complaint itself. *Khoja*, 899 F.3d at 1002. “The
 10 doctrine prevents plaintiffs from selecting only portions of documents that support their claims,
 11 while omitting portions of those very documents that weaken—or doom—their claims.” *Id.* A
 12 defendant can seek to incorporate a document into the complaint “if the plaintiff refers extensively
 13 to the document or the document forms the basis of the plaintiff’s claim.” *U.S. v. Ritchie*, 342
 14 F.3d 903, 908 (9th Cir. 2003) (citations omitted). While the “mere mention” of the existence of a
 15 document is insufficient to incorporate a document, it is proper to incorporate a document if the
 16 claim “necessarily depended” on them. *Khoja*, 899 F.3d at 1002.

17 After a defendant offers such a document, the district court can treat the document as part
 18 of the complaint, and “thus may assume that its contents are true for purposes of a motion to
 19 dismiss under Rule 12(b)(6).” *Ritchie*, 342 F.3d at 908. However, “[w]hile this is generally true,
 20 it is improper to assume the truth of an incorporated document if such assumptions only serve to
 21 dispute facts stated in a well-pleaded complaint.” *Khoja*, 899 F.3d at 1003. Indeed, using
 22 extrinsic documents to “resolve competing theories against the complaint risks premature
 23 dismissals of plausible claims that may turn out to be valid after discovery” and it is “improper to
 24 do so only to resolve factual disputes against the plaintiff’s well-pled allegations in the
 25 complaint.” *Id.* at 998, 1014.

26 **B. Analysis**

27 Defendants ask the Court to take judicial notice of or incorporate by reference the
 28 following documents:

- (1) Robinhood's publicly available webpage titled "Our 6 commitments to you," including archived versions of the webpage throughout the alleged class period (Dkt. 15-2 Ex. 1);
- (2) Robinhood's July 24, 2019 e-mails entitled "Protecting your information" (Dkt. 15-3 Ex. 2);
- (3) Robinhood's October 9-13, 2020 "Inbox Message" advising customers to "Enable Two-Factor Authentication" (Dkt. 15-4 Ex. 3);
- (4) Robinhood's October 9-13, 2020 "Push Notification" advising customers to "Enable Two-Factor Authentication to add another layer of protection to your account" (Dkt. 15-5 Ex. 4);
- (5) Robinhood's October 21-23, 2020 "Enable 2FA" follow up campaign e-mail reminding customers to enable 2FA (Dkt. 15-6 Ex. 5); and
- (6) Robinhood's October 28-29, 2020 2FA application "Card" advising customers to "Add an extra layer of protection to your account. Enable 2FA now" (Dkt. 15-7 Ex. 6).

Dkt. 16.

Plaintiffs ask the Court to take judicial notice of or incorporate by reference the following documents:

- (1) Bloomberg news article, "Robinhood Users Say Accounts Were Looted, No One to Call," dated October 9, 2020 (Dkt. 20-1 Ex. 1);
- (2) Bloomberg news article, "Robinhood Internal Probe Finds Hackers Hit Almost 2,000 Accounts," dated October 15, 2020 (Dkt. 20-2 Ex. 2);
- (3) Bloomberg news article, "Digital Thieves Are Hacking Brokerage Accounts: Is Your Money Safe?" dated October 13, 2020 (updated October 15, 2020) (Dkt. 20-3 Ex. 3);
- (4) Robinhood Customer Agreement from April 28, 2020 (Dkt. 20-4 Ex. 4); and
- (5) Robinhood Financial Privacy Notice (Dkt. 20-5 Ex. 5).

Dkt. 19.

///

///

As stated on the record at the hearing, the Court rules as follows:

Document	Ruling
Defendants' Exhibit 1 (Dkt. 15-2)	Request for judicial notice is GRANTED without any commentary or markings added to the document. Request to incorporate by reference is DENIED .
Defendants' Exhibit 2 (Dkt. 15-3)	Request for judicial notice and request to incorporate by reference are DENIED AS MOOT .
Defendants' Exhibit 3 (Dkt. 15-4)	Request for judicial notice is GRANTED . Request to incorporate by reference is DENIED .
Defendants' Exhibit 4 (Dkt. 15-5)	Request for judicial notice and request to incorporate by reference are DENIED .
Defendants' Exhibit 5 (Dkt. 15-6)	Request for judicial notice is GRANTED . Request to incorporate by reference is DENIED .
Defendants' Exhibit 6 (Dkt. 15-7)	Request for judicial notice and request to incorporate by reference are DENIED .
Plaintiffs' Exhibit 1 (Dkt. 20-1)	Request for judicial notice is GRANTED . Request to incorporate by reference is DENIED .
Plaintiffs' Exhibit 2 (Dkt. 20-2)	Request for judicial notice is GRANTED . Request to incorporate by reference is DENIED .
Plaintiffs' Exhibit 3 (Dkt. 20-3)	Request for judicial notice is GRANTED . Request to incorporate by reference is DENIED .
Plaintiffs' Exhibit 4 (Dkt. 20-4)	Request for judicial notice is GRANTED . Request to incorporate by reference is DENIED .
Plaintiffs' Exhibit 5 (Dkt. 20-5)	Request for judicial notice is GRANTED . Request to incorporate by reference is DENIED .

IV. MOTION TO DISMISS**A. Legal Standard**

Under Rule 12(b)(6), a district court must dismiss a complaint if it fails to state a claim upon which relief can be granted. In ruling on a motion to dismiss, the court may consider only “the complaint, materials incorporated into the complaint by reference, and matters of which the court may take judicial notice.” *Metzler Inv. GMBH v. Corinthian Colls., Inc.*, 540 F.3d 1049, 1061 (9th Cir. 2008) (citation omitted). In deciding whether the plaintiff has stated a claim, the court must assume the plaintiff’s allegations are true and draw all reasonable inferences in the plaintiff’s favor. *Usher v. City of L.A.*, 828 F.2d 556, 561 (9th Cir. 1987). However, the court is not required to accept as true “allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable inferences.” *In re Gilead Scis. Sec. Litig.*, 536 F.3d 1049, 1055 (9th Cir. 2008) (citation omitted).

To survive a motion to dismiss under Rule 12(b)(6), the plaintiff must allege “enough facts to state a claim to relief that is plausible on its face.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570, 127 S. Ct. 1955, 167 L. Ed. 2d 929 (2007). This “facial plausibility” standard requires the plaintiff to allege facts that add up to “more than a sheer possibility that a defendant has acted unlawfully.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678, 129 S. Ct. 1937, 173 L. Ed. 2d 868 (2009).

Courts should freely give leave to amend unless the district court determines that it is clear that the complaint’s deficiencies cannot be cured by amendment. *Lucas v. Dep’t of Corr.*, 66 F.3d 245, 248 (9th Cir. 1995). When amendment would be futile, the court may dismiss without leave to amend. *Dumas v. Kipp*, 90 F.3d 386, 393 (9th Cir. 1996).

B. Analysis

Plaintiffs allege that due to Robinhood’s failure to maintain proper industry-standard security measures, customers were needlessly exposed to the risk of data and identity theft. Dkt. 10 ¶¶ 16, 17. As a result of Robinhood’s security measures, unauthorized third parties accessed approximately 2,000 customers’ personal and financial information, customers’ funds, and control over securities positions customers purchased through Robinhood. *Id.* ¶ 18. Plaintiffs allege that Robinhood “has repeatedly neglected to fully inform customers regarding the nature and scope of

security failures and unauthorized activity.” *Id.* ¶ 20. Further, “[c]ontrary to Robinhood’s ‘commitment’ to cover losses caused by unauthorized use, Robinhood has failed to compensate millions of dollars of losses claimed by those affected by the breach.” *Id.* ¶ 22. From these allegations, Plaintiffs assert eight claims: (1) negligence; (2) breach of contract; (3) violation of the California Consumer Privacy Act; (4) violation of the Customer Records Act; (5) violation of the Consumers Legal Remedies Act; (6) violation of the right to privacy; (7) violation of the Unfair Competition Law; and (8) violation of the False Advertising Law.

Defendants assert an overarching argument that Robinhood’s computer network did not suffer a data breach and Plaintiffs fail to adequately plead that Robinhood maintained inadequate security measures. Defendants also assert arguments as to why each claim individually should be dismissed.

1. Unauthorized Access

Defendants first argue that Plaintiffs fail to allege a breach of Robinhood’s network and that Plaintiffs cannot do so, because there was no such breach. Dkt. 15 at 16. Defendants contend that “third parties were able to access customer accounts by identity theft originating outside the Robinhood system.” *Id.* at 16-17 (citing Dkt. 10 ¶ 20) (internal quotation marks omitted). Defendants further argue that “Plaintiffs plead no facts tying any account takeovers to Robinhood’s security measures.” *Id.* at 17. Without such allegations, Plaintiffs’ FAC is “too conclusory and must be dismissed.” *Id.* Defendants further argue that Robinhood has more than 13 million customers and that the number of alleged takeovers is no more than .01 percent of their customers. Dkt. 22 at 6.

In opposition, Plaintiffs argue that the FAC does allege that Robinhood used inadequate data security. Dkt. 17 at 11. Plaintiffs contend that alleging that thousands of customer accounts accessed by unauthorized users in a matter of days is “more than enough for a reasonable inference of a breach of a computer system in a data security case.” *Id.*

The Court finds that Plaintiffs’ factual allegations are sufficient to support their claims at the pleading stage. Plaintiffs allege that Robinhood “does not keep its promise to maintain the highest security standards” and “[i]ts system lacks simple and almost universal security measures”

that could “prevent unauthorized users from transferring customer funds from an account without substantial verification.” Dkt. 10 ¶ 15. Plaintiffs allege that as a result, Robinhood “negligently and illegally allowed unauthorized third-party access to approximately 2,000 customers’ personal and financial information.” *Id.* ¶ 18. Thus, at this stage of the proceedings, Plaintiffs’ allegations that unauthorized third parties were able to access approximately 2,000 Robinhood customers’ accounts and deplete their funds due to Robinhood’s security measures are sufficient. *Usher*, 828 F.2d at 561 (“On a motion to dismiss for failure to state a claim, the court must presume all factual allegations of the complaint to be true and draw all reasonable inferences in favor of the nonmoving party.”) (citation omitted). Accordingly, the Court finds that Plaintiffs have adequately alleged that a breach occurred.

2. Negligence Claim

a. Economic Loss Doctrine

Defendants argue that the economic loss rule bars Plaintiffs from recovering for any alleged account losses in tort. Dkt. 15 at 23. Defendants further argue that the exception to the economic loss rule where a special relationship exists between the parties does not apply here. *Id.* at 24. At the hearing, Defendants acknowledged that there were non-economic losses alleged, but argues that they were too vague and speculative to be redressable.

“Quite simply, the economic loss rule prevents the law of contract and the law of tort from dissolving one into the other.” *Robinson Helicopter Co., Inc. v. Dana Corp.*, 34 Cal.4th 979, 988, 22 Cal.Rptr.3d 352, 102 P.3d 268, 273 (2004). “Under the economic loss rule, purely economic losses are not recoverable in tort.” *R Power Biofuels, LLC v. Chemex LLC*, No. 16-CV-00716-LHK, 2016 WL 6663002, at *4 (N.D. Cal. Nov. 11, 2016) (internal quotation marks and citation omitted). If Plaintiffs’ harms were purely economic, the Court would then be required to reach the question of whether any exception, such as a “special relationship,” exists. *Flores-Mendez v. Zoosk, Inc.*, No. C 20-04929 WHA, 2021 WL 308543, at *3 (N.D. Cal. Jan. 30, 2021) (citing *J’Aire Corp. v. Gregory*, 24 Cal.3d 799, 804 (1979) (discussing the six-factor test for special relationship that can overcome the economic loss doctrine)).

Plaintiffs allege that their harms and losses include “the loss of control over the use of their

identity, harm to their constitutional right to privacy, lost time dedicated to the investigation of and attempt to recover the loss of funds and cure harm to their privacy, the need for future [] time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal and financial information disclosed.” Dkt. 10 ¶ 48; *see Flores-Mendez*, 2021 WL 308543, at *3 (determining that plaintiffs do not allege pure economic loss because they allege “loss of time, risk of embarrassment, and enlarged risk of identity theft”); *Bass v. Facebook, Inc.*, 394 F. Supp. 3d 1024, 1039 (“Here, plaintiff alleged his loss of time as a harm and so does not allege pure economic loss.”); *see also In re Solara Medical Supplies, LLC Customer Data Security Breach Litigation*, --- F. Supp. 3d ---, No. 3:19-cv-2284-H-KSC, 2020 WL 2214152, at *4 (S.D. Cal. May 7, 2020) (finding that plaintiffs do not allege pure economic loss because they alleged that they “lost time responding to the Breach as well as suffering from increased anxiety”); *but see Gardiner v. Walmart Inc.*, No. 20-cv-04618-JSW, 2021 U.S. Dist. LEXIS 75079, at *24 (N.D. Cal. Mar. 5, 2021) (finding that “[p]laintiff’s allegations about the value of his lost time constitutes economic loss”).

Based upon the allegations in the FAC, the Court finds that Plaintiffs do not allege solely economic loss. *See, e.g.*, Dkt. 10 ¶ 48 (alleging that Defendants’ actions “caus[ed] [Plaintiffs] harms and losses including but not limited to [] the loss of control over the use of their identity, harm to their constitutional right to privacy, lost time dedicated to the investigation of and attempt to recover the loss of funds and cure harm to their privacy, the need for future [] time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal and financial information disclosed”). Accordingly, the Court need not address whether a special relationship exists and turns to the elements of a negligence claim.

b. Negligence

To state a claim for negligence, a plaintiff must plead a duty, a breach of duty, proximate cause, and damages. *See Corales v. Bennett*, 567 F.3d 554, 572 (9th Cir. 2009).

Defendants argue that the FAC fails to adequately allege any breach of a general duty of care. Dkt. 15 at 34. Plaintiffs contend that Robinhood owed a duty to Plaintiffs because it was the custodian of their highly sensitive personal and financial information. Dkt. 17 at 13. The Court

1 agrees with Plaintiffs. Plaintiffs have sufficiently alleged that Defendants owed a duty of
 2 reasonable care to Plaintiffs. Dkt. 10 ¶ 45 (alleging that “Defendants owed a duty of reasonable
 3 care . . . based upon Defendants’ contractual obligations, custom and practice, right to control
 4 information and funds in its possession, exercise of control over the information and funds in its
 5 possession, authority to control the information and funds in its possession, and the commission of
 6 affirmative acts that resulted in said harms and losses”); *see Flores-Mendez*, 2021 WL 308543, at
 7 *4 (determining that plaintiffs have adequately alleged a duty of care); *see also Stasi v. Immediata*
 8 *Health Group Corp.*, --- F. Supp. 3d ----, No. 19cv2353 JM (LL), 2020 WL 6799437, at *7 (S.D.
 9 Cal. Nov. 19, 2020) (citing cases that found that defendants had a duty to safeguard personal
 10 information and maintain adequate security measures).

11 Plaintiffs further allege that Defendants breached their duty of care in their manner of
 12 collecting, maintaining, and controlling their customers’ sensitive personal and financial
 13 information. Dkt. 10 ¶ 46. Specifically, Plaintiffs contend that Defendants breached this duty by
 14 “stor[ing] customers’ information in an unsecure format (¶ 16), fail[ing] to require multi-factor
 15 authentication at login (¶ 20), allow[ing] unauthorized users to link bank accounts to customer
 16 accounts without verification (¶ 15), and otherwise implement[ing] lax security practices that
 17 allowed unauthorized access to Plaintiffs’ accounts (¶¶ 17, 46).” Dkt. 17 at 12-13. In *Flores-*
 18 *Mendez*, the Court reasoned that “[t]he consuming public has come to believe that internet
 19 companies, which take in their private information, have taken adequate security steps to protect
 20 the security of that information from any and all hackers or interventions.” 2021 WL 308543, at
 21 *4 (“The breach would not have occurred but for inadequate security measures, or so it can be
 22 reasonably inferred at the pleadings stage.”).

23 Third, Plaintiffs have sufficiently alleged proximate cause, alleging that “unauthorized
 24 users gained access to, exfiltrated, stole, and gained disclosure of the sensitive personal and
 25 financial information of Plaintiffs and the Class, access to the funds customers had deposited into
 26 their accounts, and control over securities positions customers purchased.” Dkt. 10 ¶ 48.

27 As to damages, Plaintiffs adequately allege damages, including “the loss of control over
 28 the use of their identity, harm to their constitutional right to privacy, lost time dedicated to the

investigation of and attempt to recover the loss of funds and cure harm to their privacy, the need for future [] time dedicated to the recovery and protection of further loss, and privacy injuries associated with having their sensitive personal and financial information disclosed.” *Id.*; see *Flores-Mendez*, 2021 WL 308543, at *4.

c. Negligence Per Se

Plaintiffs also allege that Defendants “committed *per se* breaches of said duty by negligently violating the dictates of California Civil Code sections 1798.82, *et seq.*, and 1798.100, *et seq.*, and the provisions of the California Constitution enshrining the right to privacy.” Dkt. 10 ¶ 47. “In California, there are four elements required to establish a viable negligence *per se* theory: (1) the defendant violated a statute or regulation; (2) the violation caused the plaintiff’s injury; (3) the injury resulted from the kind of occurrence the statute or regulation was designed to prevent; and (4) the plaintiff was a member of the class of persons the statute or regulation was intended to protect.” *Carson v. Depuy Spine Inc.*, 365 F. App’x. 812, 815 (9th Cir. 2010). “District courts have relied on allegations of negligence *per se* to deny Rule 12(b)(6) motions to dismiss.” *Stasi*, 2020 WL 6799437, at *12.

As discussed below, Plaintiffs plead a plausible violation of the California Consumer Privacy Act (Section IV.B.4) and their constitutional right to privacy (Section IV.B.7). It is reasonable at this stage in the litigation to determine that Plaintiffs’ alleged injuries are the injuries the California Consumer Privacy Act and constitutional right to privacy were intended to prevent and that Plaintiffs are members of the class of persons the California Consumer Privacy Act and constitutional right to privacy were intended to protect.

Accordingly, for the foregoing reasons, Defendants’ motion to dismiss Plaintiffs’ negligence claim is **DENIED**.

3. Breach of Contract Claim

To plead a claim for breach of contract, Plaintiffs must allege: “(1) the existence of a contract with Defendants, (2) their performance under that contract, (3) Defendants breached that contract, and (4) they suffered damages.” *In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 831 (N.D. Cal. 2020) (citation omitted).

Defendants contend that Plaintiffs' breach of contract claim fails because Plaintiffs' allegation that Robinhood promised to reimburse customers for account losses due to unauthorized activity is not enforceable. Dkt. 15 at 18. Defendants argue that this statement was made only after Plaintiffs opened their Robinhood accounts and after Plaintiffs Mehta's and Qian's accounts were taken over. *Id.* at 18-19. Further, Defendants contend that the statements that Robinhood is "[d]edicated to maintaining the highest security standards" and that "we take privacy and security seriously" are "not the kind of sufficiently definite promise that can support any legal claim." *Id.* at 19-21. Defendants also argue that Plaintiffs' injuries are not recoverable under a breach of contract claim because unauthorized collection of personal information does not create an economic loss and "[n]ominal damages, speculative harm, or threat of future harm do not suffice to show legally cognizable injury." *Id.* at 26 (quoting *In re Solara*, 2020 WL 2214152, at *5) (citation omitted).

Plaintiffs contend that a Robinhood spokesperson stated that "[i]f we determine that our investigation that the customer has sustained losses because of unauthorized activity, we will compensate the customer fully for those losses." Dkt. 17 at 20 (citing Dkt. 20-3 Ex. 3). Further, Plaintiffs contend that the December 30, 2020 Robinhood Customer Agreement, which is attached to the FAC as Exhibit 2, states that Robinhood "will correct any error promptly." Dkt. 17 at 20. Plaintiffs argue that this same representation was also made in the April 28, 2020 version of the Robinhood Customer Agreement, prior to the alleged unauthorized access of Mehta's and Qian's accounts, although this document is not referenced in the FAC. *Id.* They contend that this statement would "presumably [] include unauthorized transfers." *Id.* Plaintiffs also reference, in their opposition but not in the FAC, the Robinhood Financial Privacy Notice, arguing that this document also contains actionable promises. *Id.* at 21 (citing Dkt. 20-5 Ex. 5). Finally, Plaintiffs contend that they plead appreciable and actual damage, as well as future economic loss. Dkt. 17 at 26.

Plaintiffs do not sufficiently allege a breach of contract claim. First, the version of the Robinhood Customer Agreement attached to the FAC is not the Customer Agreement that was effective at the time of the alleged breach of Plaintiffs Mehta's and Qian's accounts. *See* Dkt. 10 ¶

50. Similarly, while Plaintiffs reference the Bloomberg statement and Financial Privacy Notice in their opposition for the assertion that these documents also show actionable promises, there is no specific reference to these documents in the FAC. *See* Dkt. 17 at 21. Plaintiffs have not met their burden of pleading the basis of their breach of contract claim. Accordingly, Defendants’ motion to dismiss Plaintiffs’ breach of contract claim is **GRANTED**.

4. California Consumer Privacy Act (“CCPA”) Claim

The CCPA permits “[a]ny consumer whose nonencrypted and nonredacted personal information . . . is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business’s violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action.” Cal. Civ. Code § 1798.150(a)(1). Defendants argue that Plaintiffs’ CCPA claim fails because Plaintiffs cannot allege any qualifying unauthorized disclosure or that any such disclosure was the result of a violation of “the duty to implement and maintain reasonable and appropriate security procedures and practices.” Dkt. 15 at 27. Defendants further contend that CCPA’s private right of action provision applies only to an unauthorized access of personal information from Robinhood’s network, rather than independent third-party breaches of Plaintiffs’ individual accounts. *Id.* at 28. Defendants also contend that Plaintiffs did not allege theft or disclosure of each required data element. *Id.* at 27. On the other hand, Plaintiffs contend that the California Legislature “intended for a broad range of activity or inactivity to constitute violations of the CCPA.” Dkt. 17 at 15. Further, Plaintiffs contend that courts have defined “disclosure” under CCPA to include circumstances when personal information is accessible through the internet by unauthorized persons. *Id.* at 14 (citing *Stasi*, 2020 WL 6799437, at *16).

The Court previously determined that Plaintiffs plausibly allege that a breach occurred. *See* Section IV.B.1. The Court finds *Stasi* instructive, where the parties determined that allegations that plaintiffs’ personal and medical information were accessible via the internet constitute a “disclosure” under the CCPA. *Stasi*, 2020 WL 6799437, at *16. Defendants have not met their burden of showing otherwise. Plaintiffs allege that Robinhood has customers’ “sensitive personal and financial information, including but not limited to their names, social security

1 numbers, dates of birth, mailing addresses, telephone numbers, bank account numbers, details of
 2 their income, bank account balances, financial transaction histories, credit histories, tax
 3 information, and credit scores” as well as “cell phone and mobile computing device location data,
 4 IP addresses, and Wi-Fi network data.” Dkt. 10 ¶¶ 12-13. Plaintiffs also allege that Defendants
 5 violated their duty to implement and maintain reasonable security procedures by “allow[ing]
 6 unauthorized users to view, use, manipulate, exfiltrate, and steal the nonencrypted and
 7 nonredacted personal information of Plaintiffs and other customers, including their personal and
 8 financial information.” *Id.* ¶ 58. At the pleadings stage, Plaintiffs sufficiently allege a plausible
 9 claim that their personal and financial information was subject to an unauthorized access based on
 10 violation of the CCPA. Accordingly, Defendants’ motion to dismiss Plaintiffs’ CCPA claim is
 11 **DENIED.**

12 **5. Customer Records Act (“CRA”) Claim**

13 The CRA states that “[a] person or business that conducts business in California, and that
 14 owns or licenses computerized data that includes personal information, shall disclose a breach of
 15 the security of the system following discovery or notification of the breach in the security of the
 16 data to a resident of California . . . whose unencrypted personal information was, or is reasonably
 17 believed to have been, acquired by an unauthorized person . . . in the most expedient time possible
 18 and without unreasonable delay.” Cal. Civ. Code § 1798.82(a). Similar to the CCPA claim,
 19 Defendants contend that this claim fails without any allegation of any unauthorized access to
 20 Robinhood’s computer network. Dkt. 15 at 12, 29; Dkt. 22 at 15. Further, Defendants argue that
 21 Plaintiffs fail to allege when Robinhood first learned of any incident for which it should have
 22 notified Plaintiffs sooner. Dkt. 15 at 30; Dkt. 22 at 15. Plaintiffs contend that “the Court can
 23 reasonably infer that Robinhood suffered a ‘breach of the security system’ for the purposes of the
 24 CRA” from the FAC. Dkt. 17 at 16. While not addressed in the opposition, Plaintiffs argued at
 25 the hearing that they allege in the FAC that Robinhood only disclosed the security breach after
 26 reports were leaked by anonymous sources to news outlets (Dkt. 10 ¶ 20) and that thousands of
 27 Robinhood customers attempted to contact Robinhood by email (*Id.* ¶ 4). Plaintiffs also
 28 acknowledged at the hearing that this claim can be amended.

As stated above, the Court finds that Plaintiffs plausibly allege a breach. *See* Section IV.B.1. However, the Court agrees with Defendants that Plaintiffs have not sufficiently alleged when Robinhood actually discovered that the unauthorized access took place. *See In re Yahoo! Inc. Customer Data Security Breach Litigation*, 313 F. Supp. 3d 1113, 1146 (N.D. Cal. 2018) (dismissing plaintiffs' CRA claim because plaintiffs failed to allege anything suggesting when defendants learned of the breach, which is necessary to determine whether there was unreasonable delay). Accordingly, Defendants' motion to dismiss Plaintiffs' CRA claim is **GRANTED**.

6. Consumers Legal Remedies Act ("CLRA") Claim

The CLRA prohibits "unfair methods of competition and unfair or deceptive acts or practices." Cal. Civ. Code § 1770. To state a claim under CLRA, a plaintiff must allege: "(1) a misrepresentation; (2) reliance on that misrepresentation; and (3) damages caused by that misrepresentation." *In re Sony PS3 Other OS Litigation*, 551 F. App'x 916, 920 (9th Cir. 2014). "CLRA claims are governed by the 'reasonable consumer' test, under which a plaintiff must allege that 'members of the public are likely to be deceived.'" *Id.* (quoting *Williams v. Gerber Prods. Co.*, 552 F.3d 934, 938 (9th Cir.2008)).

First, Defendants contend that this claim is subject to the heightened pleading requirements of Federal Rule of Civil Procedure 9(b), and Plaintiffs fail to adequately allege any enforceable promise. Dkt. 15 at 16, 18-22. Defendants contend that the statement "to fully reimburse direct losses that happen due to unauthorized activity that is not your fault" was never made before the alleged third-party takeovers of Plaintiffs Mehta's and Qian's accounts. *Id.* at 11, 19-20. Additionally, Defendants contend that the statements made regarding Robinhood's security commitments such as "tak[ing] privacy and security seriously" and that Robinhood is "[d]edicated to maintaining the highest security standards" are "non-actionable puffery." *Id.* at 21-22 (citing *In re Yahoo! Inc. Customer Data Sec. Breach Litig.*, No. 16-MD-02752-LHK, 2017 WL 3727318, at *26 (N.D. Cal. Aug. 30, 2017). Specifically, Defendants argue that these statements "say nothing about the specific characteristics" of Robinhood's security systems or practices. *Id.* at 22 (citing *In re Yahoo!*, 2017 WL 327318, at *26). Finally, Defendants contend that Plaintiffs' failure to allege any economic losses undermines their statutory standing to pursue a CLRA claim. *Id.* at 26.

1 Plaintiffs contend that their allegations “are more than sufficient to put Robinhood on
2 notice of the specific conduct for which relief is sought.” Dkt. 17 at 27. Plaintiffs argue that
3 “Robinhood makes specific, non-subjective guarantees of the sort courts find actionable when
4 broken,” contending that Robinhood’s guarantees are “actionable, non-puffery.” *Id.* at 21.
5 Plaintiffs point to the statements that Robinhood offers “robust security tools” and that it
6 maintains “the highest security standards,” as well as the Financial Privacy Notice which states
7 that Robinhood uses “computer safeguards and secured files and buildings.” *Id.* at 21 (citing Dkt.
8 10 ¶ 14; Dkt. 20-5 Ex. 5). Further, Plaintiffs contend that Plaintiffs sufficiently allege economic
9 loss. *Id.* at 29 (citing Dkt. 10 ¶¶ 27-29).

10 As stated on the record at the hearing, the Financial Privacy Notice is the only document
11 presented by the Parties that may contain actionable, non-puffery statements. The statements
12 Plaintiffs point to in the Privacy Policy and the 6 Commitments stating that Robinhood “take[s]
13 privacy and security seriously” and that they are “[d]edicated to maintaining the highest security
14 standards” are non-actionable puffery. “[G]eneralized, vague and unspecified assertions[]
15 constitute[] mere puffery upon which a reasonable consumer could not rely.” *Glen Holly Entm’t,*
16 *Inc. v. Tektronix Inc.*, 343 F.3d 1000, 1005 (9th Cir. 2003) (internal quotation marks and citation
17 omitted). A reasonable consumer could not rely on these statements as “specific, non-subjective
18 guarantee[s].” *In re Yahoo!*, 2017 WL 3727318, at *26. Additionally, while Plaintiffs reference
19 the Financial Privacy Notice in their opposition, as stated in Section IV.B.3, there is no reference
20 to this document in the FAC. *See* Dkt. 17 at 21. Plaintiffs have not met their burden of pleading
21 with particularity the basis of their CLRA claim. Because this conclusion requires dismissal of
22 Plaintiffs’ CLRA claim, the Court need not address Defendants’ argument regarding economic
23 losses. Accordingly, Defendants’ motion to dismiss Plaintiffs’ CLRA claim is **GRANTED**.

24 7. Right to Privacy Claim

25 “The California Constitution creates a privacy right that protects individuals’ privacy from
26 intrusion by private parties.” *In re Google Location History Litigation*, 428 F. Supp. 3d 185, 196
27 (N.D. Cal. 2019). To allege a violation of California’s constitutional right to privacy, a plaintiff
28 must allege “(1) a legally protected privacy interest; (2) a reasonable expectation of privacy under

the circumstances; and (3) conduct by the defendant that amounts to a serious invasion of the protected privacy interest.” *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1024 (N.D. Cal. 2012) (citing *Hill v. Nat’l Collegiate Athletic Ass’n*, 7 Cal. 4th 1, 35-37, 26 Cal. Rptr. 2d 834, 865 P.2d 633 (1994)). The California Supreme Court has explained that “[l]egally recognized privacy interests are generally of two classes: (1) interests in precluding the dissemination or misuse of sensitive and confidential information (‘informational privacy’); and (2) interests in making intimate personal decisions or conducting personal activities without observation, intrusion, or interference (‘autonomy privacy’).” *Hill*, 7 Cal. 4th at 35, 26 Cal. Rptr. 2d 834, 865 P.2d 633. Further, “[a]ctionable invasions of privacy must be sufficiently serious in their nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right.” *Id.* at 37.

Defendants contend that unauthorized access to Plaintiffs’ personal and financial information is not conduct by Defendants for purposes of California’s constitutional right to privacy. Dkt. 15 at 30-31. Defendants further argue that even if Plaintiffs could allege that Defendants were responsible for the unauthorized access, the unauthorized access does not rise to the level of a violation of California’s constitutional right to privacy. *Id.*

The FAC alleges that Defendants’ conduct resulted in a serious invasion of privacy due to the release of personal and financial information “including but not limited to names, social security numbers, dates of birth, mailing addresses, telephone numbers, bank account numbers, details of income, bank account balances, financial transaction histories, credit histories, tax information, credit scores, cell phone and mobile computing device location data, IP addresses, and Wi-Fi network data.” Dkt. 10 ¶ 85. As alleged, the Court finds that Plaintiffs have adequately pleaded a claim for invasion of privacy. The unauthorized access to Plaintiffs’ personal and financial information rises to the requisite level of an egregious breach of social norms. *See Richmond v. Mission Bank*, No. 1:14-cv-0184-JLT, 2015 WL 1637835, at *4 (E.D. Cal. Apr. 13, 2015) (“[I]t is indisputable that the disclosure of details regarding one’s personal finances or other financial information is a serious invasion of privacy.”) (internal quotation marks and citation omitted). Accordingly, Defendants’ motion to dismiss Plaintiffs’ invasion of privacy claim is

DENIED.

8. Unfair Competition Law (“UCL”) Claim

The UCL creates a cause of action for business practices that are: (1) unlawful; (2) unfair, or (3) fraudulent. Cal. Bus. & Profs. Code § 17200. Each “prong” of the UCL provides a separate and distinct theory of liability. *Lozano v. AT & T Wireless Servs., Inc.*, 504 F.3d 718, 731 (9th Cir. 2007). Further, to have standing to pursue this claim, plaintiffs must show that they “lost money or property” because of Defendants’ conduct. Cal. Bus. & Prof. Code § 17204; *see In re Facebook, Inc., Consumer Privacy User Profile Litig.*, 402 F. Supp. 3d 767, 804 (N.D. Cal. 2019).

a. Standing

Defendants contend that Plaintiffs have no statutory standing to assert the UCL claims, because their alleged losses are not recoverable. Dkt. 15 at 31. Additionally, Defendants argue that Plaintiffs cannot obtain restitution or injunctive relief. *Id.* To establish standing for a UCL claim, “[a] plaintiff must show he personally lost money or property because of his own actual and reasonable reliance on the allegedly unlawful business practices.” *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1071 (citing *Kwikset Corp. v. Superior Court*, 51 Cal.4th 310, 330, 120 Cal. Rptr. 3d 741, 246 P.3d 877 (2011)). However, there are “innumerable ways in which economic injury from unfair competition may be shown.” *Kwikset Corp.*, 51 Cal.4th at 323, 120 Cal. Rptr. 3d 741, 246 P.3d 877. For example, “[a] plaintiff may (1) surrender in a transaction more, or acquire in a transaction less, than he or she otherwise would have; (2) have a present or future property interest diminished; (3) be deprived of money or property to which he or she has a cognizable claim; or (4) be required to enter into a transaction, costing money or property, that would otherwise have been unnecessary.” *Id.* (citation omitted).

Plaintiffs alleged that Mehta, Qian, and Furtado have all lost thousands of dollars. Dkt. 10 ¶¶ 27-29. Further, Plaintiffs allege that they have also lost control over the use of their identity, lost time, and future economic loss. *Id.* ¶¶ 21, 27-29, 93. Additionally, Plaintiffs allege that they “made these above-market rate payments that they would not have made, or would have paid less, but for Defendants’ representations.” *Id.* ¶ 92. Thus, Plaintiffs have sufficiently alleged a loss of money or property as a result of the UCL violation.

In their opposition, Plaintiffs state that they do not intend to seek restitution under the UCL or FAL. Dkt. 17 at 30 n.2. Plaintiffs allege that unauthorized user access is an “ongoing dilemma” that “will continue into the future.” Dkt. 10 ¶¶ 19. Further, Plaintiffs allege that “Robinhood has repeatedly neglected to fully inform customers regarding the nature and scope of security failures and unauthorized activity.” *Id.* ¶ 20. Plaintiffs face a “real and immediate threat” of future injury. *In re Yahoo!*, 2017 WL 3727318, at *31 (citing *City of Los Angeles v. Lyons*, 461 U.S. 95, 111 (1983)). Accordingly, at this stage of the litigation, Plaintiffs have adequately alleged standing to seek injunctive relief under the UCL. As Plaintiffs have pleaded their UCL claim under all three prongs, the Court will address in turn whether Plaintiffs have sufficiently alleged a claim under the UCL.

b. Unlawful Prong

“The unlawful prong of the UCL prohibits anything that can properly be called a business practice and that at the same time is forbidden by law.” *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1072 (citing *Cel-Tech Commc’ns, Inc. v. L.A. Cellular Tel. Co.*, 20 Cal.4th 163, 180, 83 Cal. Rptr. 2d 548, 973 P.2d 527 (1999) (internal quotation marks omitted)). Section 17200 of the Business and Professions Code permits injured customers to “borrow” violations of other laws and treat them as unfair competition that is independently actionable. *Id.*

Plaintiffs allege that Defendants engaged in unlawful business practices in violation of the CCPA, CRA, CLRA, California Constitution right to privacy, and negligence. Dkt. 17 at 28. The Court has already considered the adequacy of Plaintiffs’ allegations as to the CCPA (Section IV.B.4), CRA (Section IV.B.5), CLRA (Section IV.B.6), California Constitution right to privacy (Section IV.B.7), and negligence (Section IV.B.2). Accordingly, the Court must **DISMISS** any claims based on violation of CRA and CLRA. *See* Sections IV.B.5-IV.B.6. On the other hand, Plaintiffs have stated a UCL claim based on CCPA, California Constitution right to privacy, and negligence, which the Court found to be sufficient pleaded. *See* Sections IV.B.2, IV.B.4, IV.B.7. Thus, Plaintiffs’ UCL claim survives to the extent it is based upon the alleged violations of CCPA, California Constitution right to privacy, and negligence, and Defendants’ motion to dismiss is **DENIED**.

c. Unfair Prong

“The UCL also creates a cause of action for a business practice that is ‘unfair’ even if not specifically proscribed by some other law.” *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1072 (citing *Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal.4th 1134, 1143, 131 Cal. Rptr. 2d 29, 63 P.3d 937 (2003)). “The UCL does not define the term ‘unfair.’ In fact, the proper definition of ‘unfair’ conduct against consumers ‘is currently in flux’ among California courts.” *Hodsdon v. Mars, Inc.*, 891 F.3d 857, 866 (9th Cir. 2018) (quoting *Davis v. HSBC Bank Nev., N.A.*, 691 F.3d 1152, 1169 (9th Cir. 2012)). “Before *Cel-Tech*, courts held that ‘unfair’ conduct occurs when that practice ‘offends an established public policy or when the practice is immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers.’” *Davis*, 691 F.3d at 1169 (citing *S. Bay Chevrolet v. Gen. Motors Acceptance Corp.*, 72 Cal. App. 4th 861, 85 Cal. Rptr. 2d 301, 316 (1999)). The balancing test in *S. Bay Chevrolet* requires the Court to “weigh the utility of the defendant’s conduct against the gravity of the harm to the alleged victim.” *Davis*, 691 F.3d at 1169 (internal quotation marks and citation omitted). In *Cel-Tech*, the California Supreme Court established a more concrete definition of “unfair,” defining it as “conduct that threatens an incipient violation of an antitrust law, or violates the policy or spirit of one of those laws because its effects are comparable to or the same as a violation of the law, or otherwise significantly threatens or harms competition.” 20 Cal. 4th at 187, 83 Cal. Rptr. 2d 548, 973 P.2d 527. Further, “any finding of unfairness to competitors under section 17200 [must] be tethered to some legislatively declared policy or proof of some actual or threatened impact on competition.” *Id.* at 186-87. While the *Cel-Tech* test did not apply to actions by consumers, “some courts in California have extended the *Cel-Tech* definition to consumer actions.” *Davis*, 691 F.3d at 1170.

Defendants argue that Plaintiffs’ claim under the unfair prong fails, because Plaintiffs cannot adequately allege a violation of California privacy laws. Dkt. 15 at 31. Plaintiffs contend that Plaintiffs’ claim under the unfair prong is “validly ‘tethered’ to the adequately pled violations of the CCPA, CRA, California Constitution, and CLRA.” Dkt. 17 at 28. Further, Plaintiffs also argue that their allegations are sufficient under the balancing test. *Id.* at 28-29. Specifically, Plaintiffs argue that they adequately alleged that Robinhood’s business practices has caused injury

to customers, “far greater than any alleged countervailing benefit.” *Id.* At the motion to dismiss stage, the Court cannot say that the benefits from Robinhood’s business practices of allegedly emphasizing growth and profit over protecting their customers’ personal and financial information and failing to implement industry-standard security measures outweighs the harm. *See In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d at 844; *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1073 (“While the benefits of Apple’s conduct may ultimately outweigh the harm to consumers, this is a factual determination that cannot be made at this stage of the proceedings.”). Accordingly, Defendants’ motion to dismiss on the unfair prong of the UCL is **DENIED**.

d. Fraudulent Prong

“In order to state a cause of action under the fraud prong of the UCL, a plaintiff must show that members of the public are likely to be deceived.” *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1073 (citing *Schnall v. Hertz Corp.*, 78 Cal. App. 4th 1144, 1167, 93 Cal. Rptr. 2d 439 (2000)). “The challenged conduct ‘is judged by the effect it would have on a reasonable consumer.’” *Davis*, 691 F.3d at 1169 (quoting *Puentes v. Wells Fargo Home Mortg., Inc.*, 160 Cal. App. 4th 638, 72 Cal. Rptr. 3d 903, 909 (2008)). Rule 9(b)’s heightened pleading requirements apply to UCL claims under this prong. *Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1125 (9th Cir. 2009). Thus, claims under this prong must allege “an account of the time, place, and specific content of the false representations as well as the identities of the parties to the misrepresentations.” *Swartz v. KPMG LLP*, 476 F.3d 756, 764 (9th Cir. 2007) (internal quotation marks and citation omitted).

Defendants make the same arguments for the fraud prong that they make regarding Plaintiffs’ CLRA claim. *See* Section IV.B.6. Here, Plaintiffs have not met their burden of pleading with particularity the basis of their UCL claim under the fraudulent prong. As stated in Section IV.B.6, the Financial Privacy Notice is the only document presented by the Parties that may contain actionable, non-puffery statements, which is not referenced in the FAC. As alleged in the FAC, there are no statements by which a reasonable consumer would be likely to be deceived. Accordingly, Defendants’ motion to dismiss on the fraudulent prong of the UCL is **GRANTED**.

////

9. False Advertising Law (“FAL”) Claim

California's False Advertising Law makes it unlawful for any person to “induce the public to enter into any obligation” based on a statement that is “untrue or misleading, and which is known, or which by the exercise of reasonable care should be known, to be untrue or misleading.” Cal. Bus. & Prof. Code § 17500. “Whether an advertisement is ‘misleading’ must be judged by the effect it would have on a reasonable consumer.” *Davis*, 691 F.3d at 1161-62 (citing *Williams*, 552 F.3d at 938). “A reasonable consumer is the ordinary consumer acting reasonably under the circumstances.” *Id.* at 1162 (internal quotation marks and citation omitted). “In applying this test, we are mindful that whether a business practice is deceptive will usually be a question of fact not appropriate for decision on a motion to dismiss.” *Id.* (citing *Williams*, 552 F.3d at 938) (internal quotation marks omitted).

Defendants make similar arguments for the FAL claim that they make regarding Plaintiffs’ UCL claim. *See* Section IV.B.8. While Plaintiffs have adequately alleged a “real and immediate threat” of injury from Defendants, Plaintiffs have not met their burden of pleading with particularity the basis of their FAL claim. Like Plaintiffs’ CLRA claim (Section IV.B.6) and UCL claim under the fraudulent prong (Section IV.B.8.d), the FAC does not reference the Financial Privacy Notice. As alleged in the FAC, there are no statements by which a reasonable consumer would have been misled to enter into any obligation. Accordingly, Defendants’ motion to dismiss Plaintiffs’ FAL claim is **GRANTED**.

V. CONCLUSION

For the reasons stated above, the Court **GRANTS IN PART AND DENIES IN PART** Defendants’ motion to dismiss pursuant to Rule 12(b)(6). Specifically, Defendants’ motion to dismiss Plaintiffs’ claims for negligence, violations of the CCPA, constitutional right to privacy, and unlawful and unfair prongs of the UCL are **DENIED**. Defendants’ motion to dismiss Plaintiffs’ claims against Defendants for breach of contract, violations of CRA, CLRA, fraudulent prong of the UCL, and FAL are **GRANTED WITH LEAVE TO AMEND**.

Plaintiffs may file an amended complaint by **May 20, 2021**. Plaintiffs may not add new causes of action or parties without leave of the Court or stipulation of the parties pursuant to

Federal Rule of Civil Procedure 15. Failure to cure the defects identified by this Order will be subject to dismissal with prejudice.

SO ORDERED.

Dated: May 6, 2021


SUSAN VAN KEULEN
United States Magistrate Judge

United States District Court
Northern District of California